一、环境准备：

VPN 设备：

1. 必须是超级管理员在操作

2. 与 LDAP 服务器网络和端口能通信

LDAP 服务器

1. 组织结构要清晰有条序，便于维护

2. 保证链接地址，管理员密码，搜索根路径等参数正确无误

二、对接 LDAP 外部认证服务器

1.“SSLVPN 设置”—“认证设置”—“主要认证”中的 LDAP 认证点击设置

2.添加 LDAP 服务器，填写相对应的参数

注释：

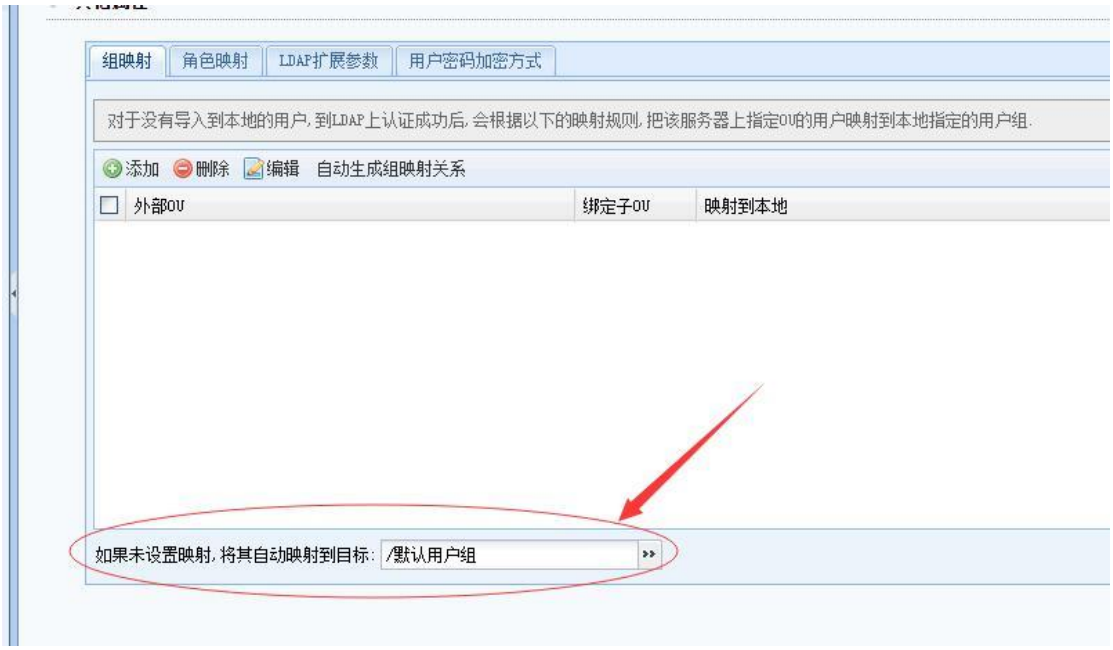
a. LDAP 服务器的 IP 地址和端口，端口默认 389，根据实际情况调整

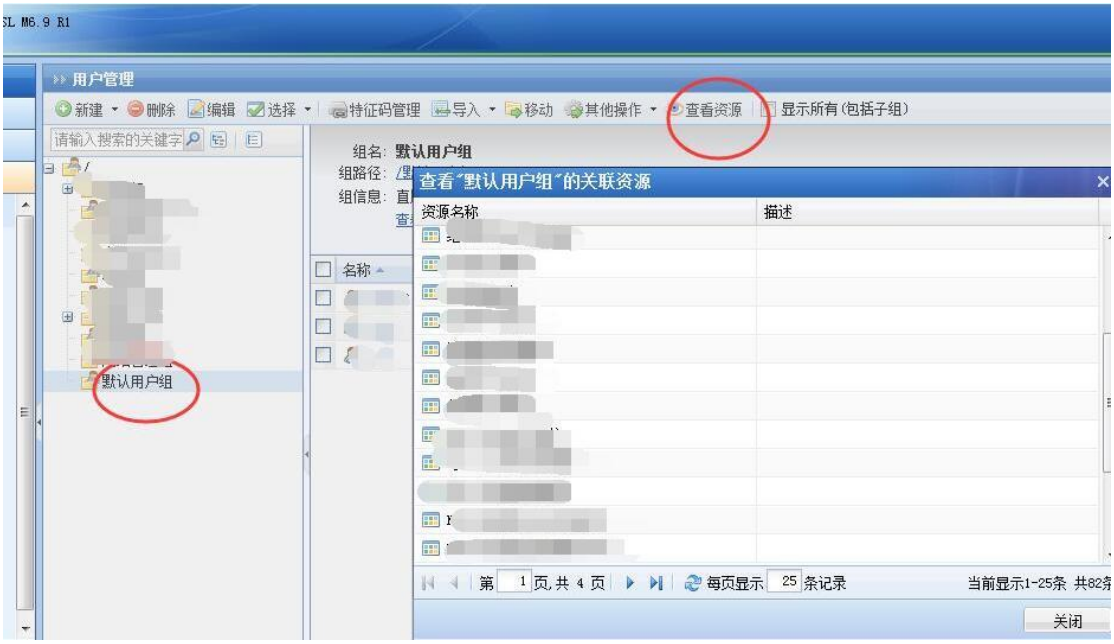
b. LDAP 服务器的管理员账号，不一定是超级管理员，拥有足够的读权限即可。一般有两种格式 administrator@sfxu.com 或者 cn=Manager,dc=ca,dc=gxtc,dc=edu,dc=cn

c. 确保需要进行认证的用户在组织结构里，如 OU，不然会认证失败，直接填写路径或者可以在搜索入口点击选择

3. 因为客户是 OPENLDAP 类型的第三方服务器，所以服务器类型选择 LDAP Server

4.其他属性无特殊需求则保持默认，不用设置组映射和角色映射，但要注意一点，LDAP 服务器上的用户都是自动映射到默认用户组，享有默认用户组所拥有的资源和角色权限





5.【注意】以上所有配置配置完成后，注意保存，并点击右上角的立即生效。

三.经验排错

1.过程描述：

之前我填写参数的时候，按照客户给的参数原原本本地填了上去发现用户登录 VPN 时提示用户名密码错误，但用同样账号密码登录内网资源是正常的，联系 400 抓包发现两端的 MD5 加密方式不一样，最后确定需要打定制包才能满足此需求。后面技术专家来帮我处理发现应该不用定制即可满足，是搜索入口的格式写得不对，把范围限制的太小了，所以无法搜索到用户，也无法完成认证。把搜索范围定义为全部根组即可!

2.测试验证

a. 登录 VPN 失败

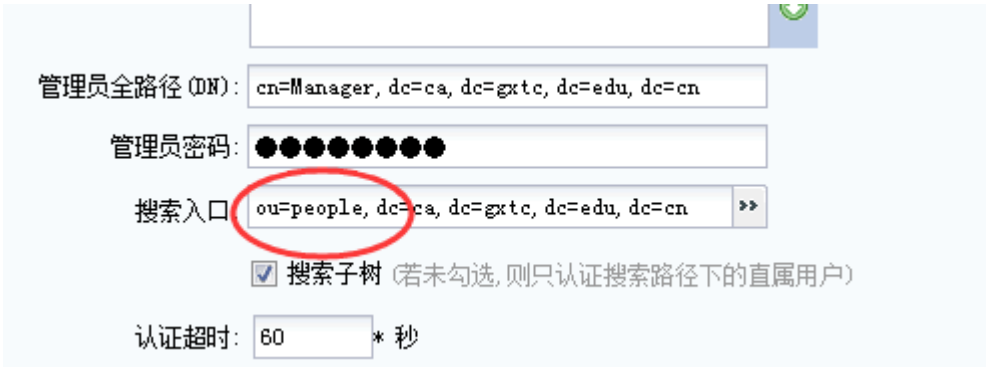
b. 在内网登录资源用相同账户能正常登录

c. 抓包数据流

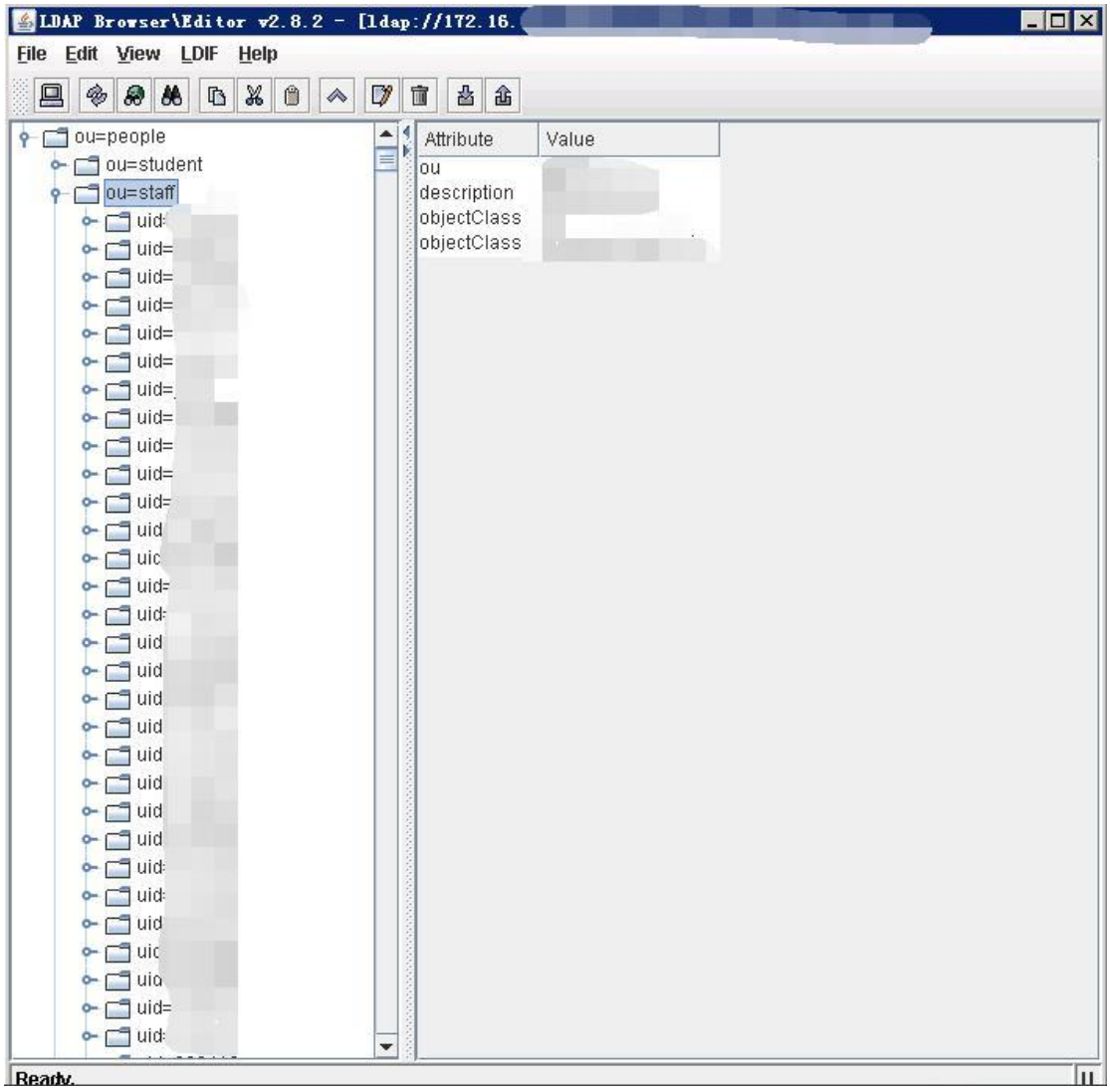
```
    objectName: uid=991086,ou=staff,ou=people,dc=ca,dc=gxtc,dc=edu,dc=cn
  ▾ attributes: 5 items
    ▸ PartialAttributeList item objectClass
    ▸ PartialAttributeList item uid
    ▸ PartialAttributeList item cn
    ▸ PartialAttributeList item lastTime
    ▾ PartialAttributeList item userPassword
        type: userPassword
      ▾ vals: 1 item
          AttributeValue: {MD5}3Eg+gKegvZ73HYz5c2c5JA==
[Response To: 8]
[Time: 0.001489000 seconds]

    version: 3
    name: uid=991086,ou=staff,ou=people,dc=ca,dc=gxtc,dc=edu,dc=cn
  ▾ authentication: simple (0)
      simple dc483e80a7a0bd9ef71d8cf973673924
[Response In: 12]
```

d. 调整配置

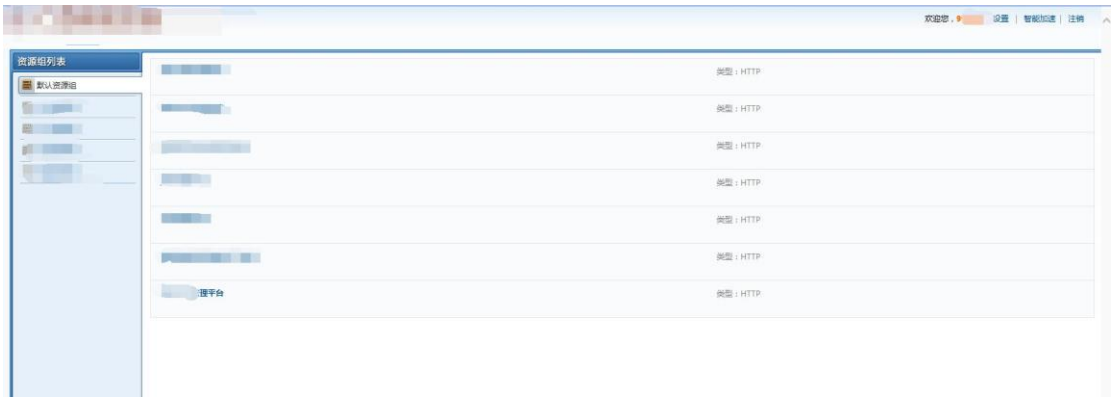


e. LDAP 服务器里面的组织结构


LDAP Browser\Editor v2.8.2 - [ldap://172.16.
File Edit View LDIF Help
ou=people
ou=student
ou=staff
Attribute
Value
ou
description
objectClass
objectClass
Ready

f. 调整后的效果


登录SSL VPN
正在检测登录信息...
登录



四．单点登录

SSL VPN 的单点登录主要分为两类：

i. 自动填表：

用户在登录 SSL 控制台以后，需要借助单点登录助手在 WEB 页面或应用程序登录页面录制单点登录；

自动填表的单点登录功能支持所有 WEB 应用，TCP 应用 ，L3VPN 和远程应用的所有 B/S 和 C/S 应用。

i. 自动构建参数：

用户在录制 SSL 单点登录的时候，不使用单点登录助手，而是手动填写相应单点登录各个参数信息；

自动构建参数的单点登录方式只支持 WEB 应用，TCP 应用，和 L3VPN

的 HTTP，HTTPS 应用。

1. 配置思路

- ✧ SSL VPN 设备开启单点登录功能序列号
- ✧ 添加相应的资源，启用“单点登录”，勾选“自动填表”方式
- ✧ 下载单点登录工具和单点登录脚本
- ✧ 使用单点登录工具进行录制
- ✧ 单点登录工具录制完成后，上传单点登录脚本到设备里
- ✧ 设置“角色授权”，将资源和用户关联起来
- ✧ 用户登录 SSL VPN，直接点击资源链接登录到内部资源

2. 配置截图

a. 查看是否有单点登录序列号授权

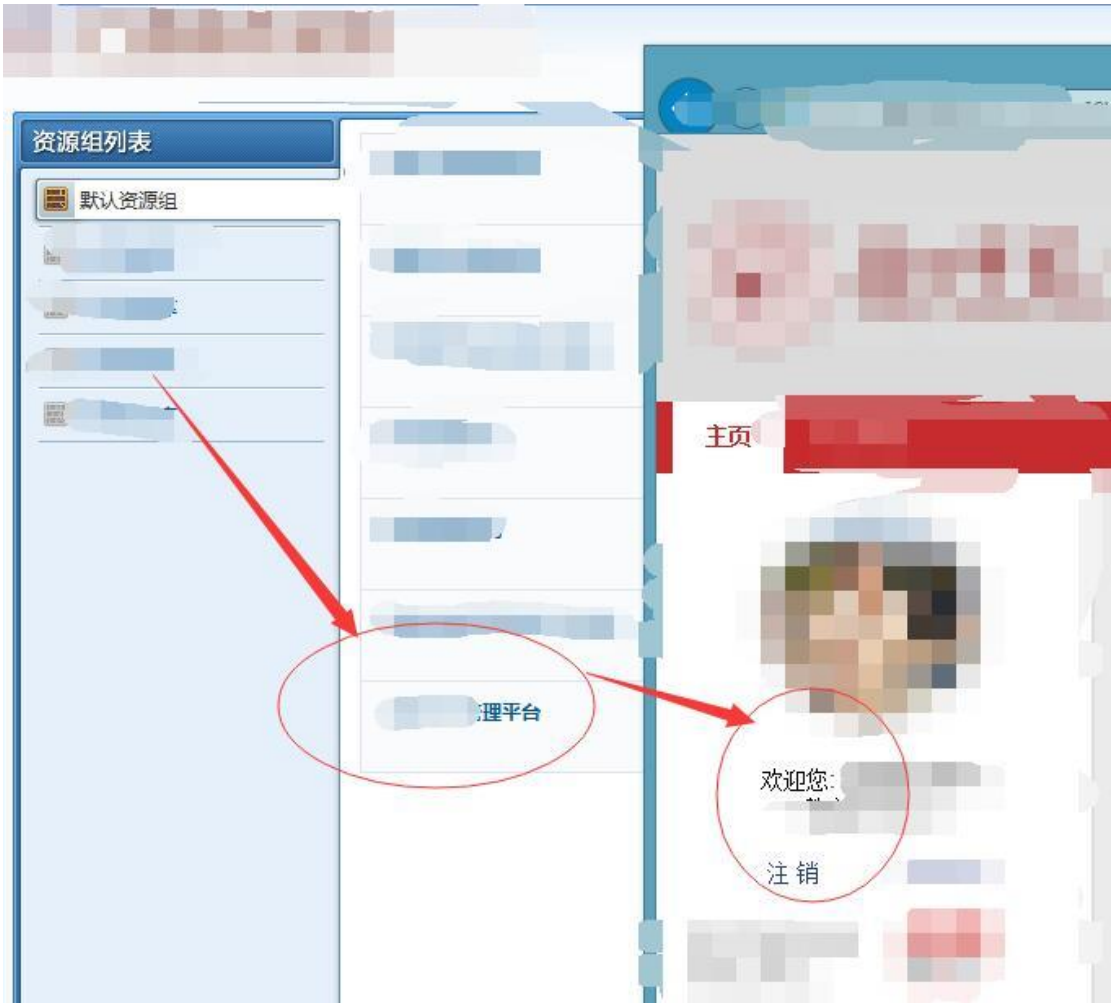
b. 新建 TCP 应用资源，勾选单点登录，登录方法为“自动填表”

c. 下载单点登录录制助手和配置文件安装

d. 上传录制好的文件到设备，记住先“保存”再点击右上方的“立即生效”

e. 编辑角色，用户和资源三者相关联起来

f. 测试用户登录 vpn，直接点击内网资源即可完成自动登录



3．注意事项

1.在录制的过程中，放大镜一定要对准用户名和密码框，如果录制完成后发现无法提交用户名密

码，尝试多录制几次，可能是没有对准

2.在录制完成后，点击资源发现用户名密码已经填上了，但是没有自动登录，此时需要检查两点

A ： 登录按钮是否录制错误，尝试重新录制登录按钮

B ：检查一下是否勾选了自动提交，没有勾选则勾选上保持单点登录配置文件重新上传

3.录制完成，打开资源发现显示的用户名密码不是想要的但却又不能

修改，检查以下两点

A ： 设备控制台单点登录处是否勾选了允许修改用户名密码

B ：在录制单点登录时用户名密码是否选择的指定值，如果是指定值则无法修改

4.需要录制的界面有验证码，无论如何录制都不行

由于验证码是随机变化的，所以无法做到自动提交，有验证码的页面最多可以做到提交用户名密码，无法自动提交